IN THE UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF MISSOURI
WESTERN DIVISION

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
	)	
v.	)	Criminal Action No.
	)	10-00328-01-CR-W-DW
MICHAEL LARSON,	)	
	)	
Defendant.	)	

REPORT AND RECOMMENDATION TO DENY DEFENDANT'S MOTION TO SUPPRESS EVIDENCE

Before the court is defendant's motion to suppress evidence seized from his home pursuant to a search warrant on the grounds that (1) the affidavit willfully omits critical and significant information known to the affiant that if revealed would have resulted in denial of the warrant, and (2) the affidavit does not establish probable cause that child pornography would be found on defendant's computer. I find that there was no material omission and that the search warrant was supported by probable cause. Therefore, defendant's motion to suppress should be denied.

I. BACKGROUND

On October 8, 2009, TFO Amanda Jatkowski in Springfield, Missouri, used the internet file-sharing application LimeWire to perform a search for shared files using terms and phrases commonly associated with child pornography. Her search argument returned a "host," or computer, with an IP ("internet protocol") address of 99.31.55.168 as having shared files with such terms

and phrases included in file names or file descriptions. Using LimeWire, TFO Jatkowski was able to query the target host for all shared files, of which 93 were present. Of the 93 shared files, TFO Jatkowski downloaded 31 and determined that all 31 contained child pornography.

Using commands widely known to IP professionals, TFO Jatkowski was able to determine that the IP address 99.31.55.168 had been assigned by AT&T Internet Services. On October 14, 2009, an administrative subpoena was served on AT&T Internet Services, who responded on October 21 with the name, address, phone number and email address of the subscriber of the internet service. The subscriber was identified as Angela Pennington at 1401 South Osage Street, Independence, Missouri.

On October 12, 2009, TFO Jeffrey Elliott, in Oklahoma City, using the same LimeWire file-sharing application as that used by TFO Jatkowski, performed a similar search using the term “Witch Nudist”, a phrase commonly associated with child pornography. His search returned files that were being shared by a host with an IP address of 75.54.75.211. A query of all shared files on the host returned 76 files. Of those, nine were downloaded, opened and determined to be child pornography. The following day, an administrative subpoena was served on AT&T Internet Services who had assigned IP address 75.54.75.211. On October

21, 2009, AT&T responded, indicating that the subscriber at the time of the downloads was Angela Pennington, 1401 South Osage Street, Independence, Missouri.[1]

---

[1] Many of the terms used in the affidavit and pleadings may not be fully understood by those with little exposure to the argot of digital age. The 15-page affidavit includes not only the above description of the investigation, but definitions, a background on computers and child pornography, the specifics of search and seizure of computer systems, how computers are searched, etc. The following paragraphs are an attempt to present a succinct clarification of how the simultaneous investigation by TFO Jatkowski and TFO Elliott led to 1401 South Osage in Independence, Missouri.

What is Limewire? Peer to peer (P2P) file sharing became a cultural phenomenon in 1999 with the advent of Napster, which was strictly a music-sharing site. The following year the P2P application LimeWire was released, followed by several others such as KaZaa, Morpheus, BearShare, etc. All were based on the Gnutella client developed by Nullsoft, which was acquired by AOL in 2000. In 2001 Napster was ordered to shut down due to copyright violations. Over the ensuing years virtually all of the Gnutella clients either shut down or adopted a "for pay" business model. An alternative to Gnutella – BitTorrent – has filled the file-sharing void, though in the last few years legitimate media sites such as iTunes and NetFlix have made available an enormous library of music, film, books and other media at low cost, putting file sharing sites based on copyright infringement increasingly on the fringe of polite society. While Napster was strictly a music-sharing site, the Gnutella clients were capable of sharing images, movies, software, published materials and so on. All that is needed to obtain and share files is an internet connection coupled with a client such as LimeWire. Once LimeWire is installed, the user can enter a search term into LimeWire, which sends the request across the internet to a peer also running a Gnutella client, which will forward that query to any peers it is connected to, and so on. The peers that are sharing files that conform to the search argument will respond back to the originating peer with its IP address, filename, file size and other detail. Depending upon the search argument, there may be many thousands of peers with the same file or like files, or few to none if the search was for something more arcane. Once the search is complete, the user can select a file from the list and choose to download it to his

On November 9, 2009, Special Agent Michael Daniels obtained a federal search warrant for 1401 South Osage Street, Independence, Missouri -- a residence shared by defendant and his girl friend, Angela Pennington. The warrant was executed the following day. Three computers were seized, two of which had internet connection. At the scene, defendant and his live-in girl friend both identified the computer containing child pornography as defendant's computer.

On November 19, 2010, an indictment was returned charging

---

computer. Additionally, the user can query the remote PC for all files that are being shared. These are the actions TFOs Jatkowski and Elliott performed to discover child pornography stored on the PC at Angela Pennington's home in Independence.

How could the same computer have different IP addresses at different times? Computers communicating on the internet are assigned a unique internet protocol (IP) address for the duration of their connection to the internet. There is a finite number of IP addresses available under the present internet architecture -- approximately 4.3 billion. These addresses are divided up by international agreement into regional divisions, which then are further divided into pools of addresses used by internet service providers (ISPs), such as AT&T, for assignment to subscribers. Both because of the address limit and the nevertheless large number of addresses to be managed, provisions had to be made within the architecture to account for this limitation. Two of these provisions are known as Network Address Translation (NAT) and Dynamic Host Configuration Protocol (DHCP). NAT overcomes the address limit by providing for the use of private, non-routable IP addresses from within a domain, while DHCP provides a means of providing an IP address to a host as needed, rather than having that address statically assigned, which would effectively remove that address from the available pool. NAT does not have a particular bearing on this case. DCHP, however, answers the question as to why on October 8, 2009, the computer responding to TFP Jatkowski's LimeWire search had IP address 99.31.55.168, while the same computer responding to TFO Elliott's LimeWire search had IP address 75.54.75.211 four days later.

defendant with one count of attempted receipt of child pornography over the internet, in violation of 18 U.S.C. § 2252(a)(2), two counts of attempted distribution of child pornography over the internet, in violation of 18 U.S.C. § 2252(a)(2), one count of receiving child pornography over the internet, in violation of 18 U.S.C. § 2252(a)(2), and one count of possessing child pornography, in violation of 18 U.S.C. § 2252(a)(4).

On February 25, 2011, defendant filed a motion to suppress (document number 18) arguing that there was "less than a 10% chance that the contraband [child pornography] was at the subscriber residence on the subscriber's computer", yet police were able to get a search warrant because the issuing judge was not made aware of this fact. Attached to his motion is an affidavit of forensic expert Greg Chatten, an affidavit of Sprint Corporation IT Senior Manager Hardy Medlin, administrative subpoenas issued to AT&T, an internet article from Australia on the dangers of WiFi, an article from 2007 Washington Post on the dangers of open WiFi, and the search warrant and supporting affidavit. On March 11, 2011, the government filed a response (document number 21) in opposition. On April 25, 2011, defendant filed supplemental citations of authority and evidence in support of his motion for a Franks hearing (document number 31).

II. FRANKS HEARING/PROBABLE CAUSE

Defendant argues that AT&T should have been the initial possible suspect, and that no further investigation was done to determine if the child pornography passed through defendant's computer to another party through open wireless network (WiFi). In other words, defendant believes that the issuing judge was duped into thinking it more likely than it really was that defendant's residence held the computer that downloaded the child pornography -- rather, it was more likely that either (1) an employee of AT&T downloaded it; or (2) someone essentially parked near defendant's residence with a laptop and accessed the internet through defendant's non-secure internet service,[2] downloaded child pornography, and then left the scene. This is the material omission which, defendant argues, requires a Franks hearing.

In Franks v. Delaware, 438 U.S. 154 (1978), the Supreme Court defined a limited exception to the presumptive validity of an affidavit supporting a search warrant application. Under Franks v. Delaware, if the government intentionally includes material false statements in its warrant affidavits or includes material false statements with reckless disregard for the truth

[2]Notably, defendant does not actually allege that his internet was non-secure.

that is the legal equivalent of an intentional falsehood, the court must set aside those statements and then review the remaining portions of the affidavit to see if what remains is sufficient to establish probable cause. United States v. Ozar, 50 F.3d 1440, 1443 (8th Cir.), cert. denied, 516 U.S. 871 (1995); United States v. Garcia, 785 F.2d 214, 222 (8th Cir.), cert. denied, 475 U.S. 1143 (1986). Defendant bears the burden of proving the intentional or reckless inclusion of false statements in a warrant affidavit. Id. at 222. The same analysis applies to omissions of fact, i.e., the defendant must show that the affiant intentionally or recklessly omitted material facts thereby making the affidavit misleading, and that the affidavit, if supplemented by the omitted information, could not support a finding of probable cause. United States v. Humphreys, 982 F.2d 254, 259 n.2 (8th Cir. 1992).

An evidentiary hearing is not warranted unless the defendant makes a strong initial showing of "deliberate falsehood or of reckless disregard for the truth." Franks v. Delaware, 438 U.S. at 171; United States v. Freeman, 625 F.3d 1049, 1052 (8th Cir. 2010). The critical step in a Franks v. Delaware analysis is to determine whether the warrant affidavit, corrected for any false statements and omissions, is sufficient to show probable cause. United States v. Ozar, 50 F.3d at 1446.

Other courts have addressed the very same argument proposed by defendant, and those courts have rejected defendant's position. In United States v. Carter, 549 F. Supp. 2d 1257 (D. Nev. 2008), law enforcement authorities identified an IP address associated with the attempted downloading of child pornography, served an administrative subpoena on the internet service provider which issued that IP address, obtained the name and address of the subscriber who used that IP address at the time the attempt was made to download child pornography, and then verified that name and address through DMV and utility records. This information was included in an affidavit for a warrant to search the residence for evidence of child pornography. The defendant in that case moved to suppress the evidence, arguing that evidence that an IP address was used to download child pornography, combined with evidence regarding the IP address subscriber's identity and residential address, was insufficient to establish probable cause to believe that evidence of child pornography would be found at the subscriber's residence. The court disagreed:

> In deciding whether the Defendant has made a sufficient threshold showing to warrant a Franks evidentiary hearing, the Court assumes that the factual information set forth in Mr. Mare's and Mr. Tobin's affidavits is accurate. The article on the FBI website also verifies that an outsider can use a subscriber's wireless connection and IP address to gain access to the Internet and, among other things, use that connection and IP address to either send or receive

> child pornography. The fact that an outside computer user can gain access to the Internet through the Internet service subscriber's wireless connection and IP address, with or without his knowledge, or that computer users can use software to "spoof" another person's assigned IP address or MAC address, are certainly possibilities that diminish the likelihood that the Internet transmission emanated from the subscriber's premises.
>
> The Court nevertheless agrees with Perez[3] that even if the information set forth in Mr. Mare's and Mr. Tobin's affidavits had been included in Agent Flaherty's affidavit, there would still have remained a likelihood or fair probability that the transmission emanated from the subscriber's place of residence and that evidence of child pornography would be found at that location. The Defendant, therefore, has not met his initial burden to show "that the 'affidavit, once corrected and supplemented,' would not 'provide . . . a substantial basis for concluding that probable cause existed' to search defendant's residence." United States v. Jawara, 474 F.3d at 582, quoting Stanert.[4] Additionally, unlike the circumstances in Stanert, supra, where the omitted information would have clearly negated probable cause, the omissions in this case do not support an inference that they were made intentionally to mislead the Court or with reckless disregard for the truth.

Id. at 1268-69.

In United States v. Hibble, 2006 WL 2620349 (D. Ariz. 2006), the defendant argued that he used an unsecured wireless router to access the internet, which allows anyone who has WiFi software to access the defendant's IP address. "This is the type of technology that is available in coffee shops like Starbucks, which allows any laptop user to use the Starbucks' IPA." The Defendant in Hibble argued that the child pornography files could

---

[3]United States v. Perez, 484 F.3d 735 (5th Cir. 2007).

[4]United States v. Stanert, 762 F.2d 775 (9th Cir. 1985).

have been downloaded from another computer that was accessing the defendant's IP address and that law enforcement officers "should have confirmed that it was in fact Defendant's activity emanating from the Defendant's computer." As was the case in United States v. Carter, discussed above, the court held that the government was not required to obtain potentially dispositive information to put in its affidavit of probable cause for a warrant.

> At the time of her affidavit of probable cause, SA Andrews had no way of knowing that Defendant was using a wireless router. This was discovered as a result of the search.
>
> The Government is not required to obtain potentially dispositive information in its affidavit of probable cause. See United States v. Gourde, 440 F.3d 1065, 1073 n. 5 (9th Cir. 2006) ("See: United States v. Miller, 753 F.2d 1475, 1481 (9th Cir. 1985) (holding that an affidavit supported probable cause even though '[i]ndependent verification could have been easily accomplished in this case and the officers failed to take these simple steps'); United States v. Ozar, 50 F.3d 1440, 1446 (8th Cir. 1995) ('[T]he magistrate judge erred in focusing his Franks v. Delaware analysis on what the FBI could have learned with more investigation'); United States v. Dale, 991 F.2d 819, 844 (D.C. Cir. 1993) (noting that 'failure to investigate fully is not evidence of an affiant's reckless disregard for the truth' and that 'probable cause does not require an officer to . . . accumulate overwhelming corroborative evidence.')"
>
> Here, SA Andrews's affidavit was based on her peer-to-peer search of the internet using a term she knew to be associated with child pornography that discovered files labeled as child pornography available for sharing at an IPA registered to the Defendant. She downloaded and opened two files, verifying that the files available at this IPA depicted child pornography. As noted in the R & R, "a magistrate judge is only required to answer the 'common-sense, practical question of whether there is probable cause to believe that contraband or evidence is located in a particular place before issuing a search warrant."

* * * * *

> . . . [T]he warrant was supported by probable cause because there was a fair probability that evidence of child pornography would be found on the computer located at the other end of the IPA. There is no showing to warrant a Franks hearing. Defendant's myriad of explanations are more suited to being raised as a defense at trial.

Id. at *3-4.

Here, defendant attempts to persuade the court that there was only a ten percent chance that the child pornography downloaded through an IP address assigned to defendant's computer would actually be found on defendant's computer. I disagree. The possibility that an AT&T employee or someone sitting in defendant's driveway downloaded the child pornography certainly exists -- but not to the extent that it destroys the probable cause to believe the child pornography would indeed be found on defendant's computer.[5]

---

[5]Defendant's supplemental citations of authority do not change my opinion. In that document defendant describes an article about a man in Buffalo, New York, whose home was the subject of a search warrant. It was later learned that the man's neighbor had downloaded the child pornography. The article states that investigators "could have taken an extra step before going inside the house and used a laptop or other device outside the home to see whether there was an unsecured signal" which could have raised the possibility that someone else was responsible for the downloads. I find that the authority offered in defendant's supplemental citations does not change my analysis, and I note also that using defendant's proffered argument, one would essentially shield himself from search warrants by maintaining open WiFi. I am not saying that further investigation should be discouraged or that the chances of people being wrongly suspected could get out of hand. I am simply saying at this point that the article presented by defendant in

Probable cause to issue a search warrant exists when an affidavit sets forth sufficient facts to justify a prudent person in the belief that there is a fair probability that contraband or evidence of a crime will be found in a particular place. Illinois v. Gates, 462 U.S. 213, 238 (1983); Brinegar v. United States, 338 U.S. 160 (1949); United States v. Reivich, 793 F.2d 957, 959 (8th Cir. 1986). A determination whether probable cause has been established involves a practical, common-sense evaluation of the totality of the circumstances. Illinois v. Gates, 462 U.S. at 238; United States v. Reivich, 793 F.2d at 959. It is unimportant whether individual corroborating facts appear to exemplify innocent or guilty activities; rather, it is how these facts fit together in the entirety which concerns a reviewing court. United States v. Robinson, 756 F.2d 56, 59-60 (8th Cir. 1985). If a common-sense decision based on all the surrounding circumstances demonstrates a fair probability that contraband or evidence of a crime will be found in a certain place, then issuance of a search warrant is proper. Illinois v. Gates, 462 U.S. at 238; United States v. Rich, 795 F.2d 680, 682 (8th Cir. 1986).

---

his supplemental brief does not persuade me that a Franks hearing is in order or that the search warrant's probable cause is in question.

Considering the totality of the circumstances, I find that the affidavit in support of the search warrant in this case establishes probable cause that child pornography would be found on a computer in defendant's residence. The affidavit indicates that two agents conducting independent investigations learned that child pornography had been downloaded by IP addresses that had been assigned to the computer in defendant's house at the time the child pornography was downloaded. It describes the process of peer-to-peer file sharing and how child pornography is stored on computers. It describes how seized computers are searched by qualified computer experts. It describes the search procedure of electronic data. And it describes characteristics common to individuals involved in the distribution, receipt, or possession of child pornography based on the knowledge, experience, and training of the affiant and other law enforcement officers involved in investigating these crimes. Those characteristics include the retaining of child pornography on computers and in hard copy form in their residences for many years, and the maintenance of correspondence from other child pornography distributors/collectors.

This information justifies a prudent person in the belief that there is a fair probability that child pornography would be found on a computer in defendant's residence. The fact that

someone could have sat outside defendant's residence with a laptop and downloaded child pornography certainly exists, but it does not negate the "fair probability" that someone inside the house downloaded that material. Defendant argues that law enforcement officers should have sat outside the residence with a laptop to see if the internet was secure or not before applying for a search warrant; however, defendant never even claims that his internet was not secure. Law enforcement officers are not required to rule out every other possibility before requesting a search warrant to further their investigation. However, I find that even if the affidavit had included the possibility that an AT&T employee or person outside defendant's residence with a laptop could have downloaded the child pornography using defendant's IP address, the affidavit would still have established probable cause that child pornography would be found on a computer inside defendant's residence.

III. CONCLUSION

Based on all of the above, I find that (1) defendant has failed to meet his burden of proving the intentional or reckless omission of material information in the warrant affidavit, and (2) with or without the information defendant believes should have been included in the affidavit, it establishes probable cause to believe that child pornography would be found on a

computer inside defendant's residence. Therefore, it is

RECOMMENDED that the court, after making an independent review of the record and the applicable law, enter an order denying defendant's motion for a Franks hearing and to suppress the evidence seized from his residence during execution of the search warrant.

Counsel are advised that, pursuant to 28 U.S.C. § 636(b)(1), each has ten days from the date of this report and recommendation to file and serve specific objections.

/s/ Robert E. Larsen
ROBERT E. LARSEN
United States Magistrate Judge

Kansas City, Missouri
August 1, 2011